Towards a Computer Network Operations (Information Assurance) Taxonomy

Bill Mandrick

Data Tactics Corporation

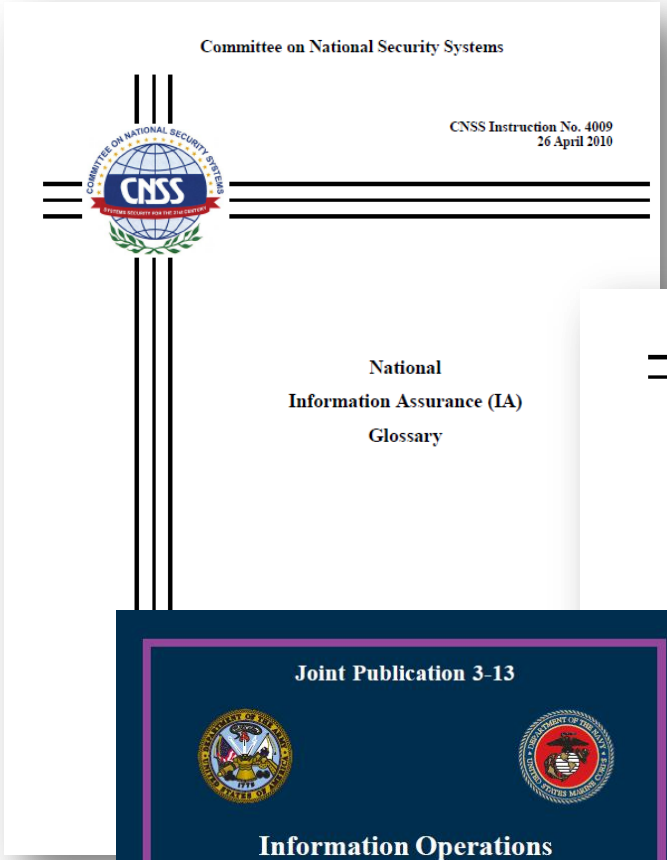
02 January 2014

Outline

- Authoritative Sources
- Well Formed Taxonomies
- Integrating Taxonomies
  - Creating Integrated Diagrams
  - Enhanced Situational Awareness
  - Knowledge Management
- Computer Network Operations (CNO) Use Case

Contact: Bill Mandrick
wmandrick@data-tactics.com

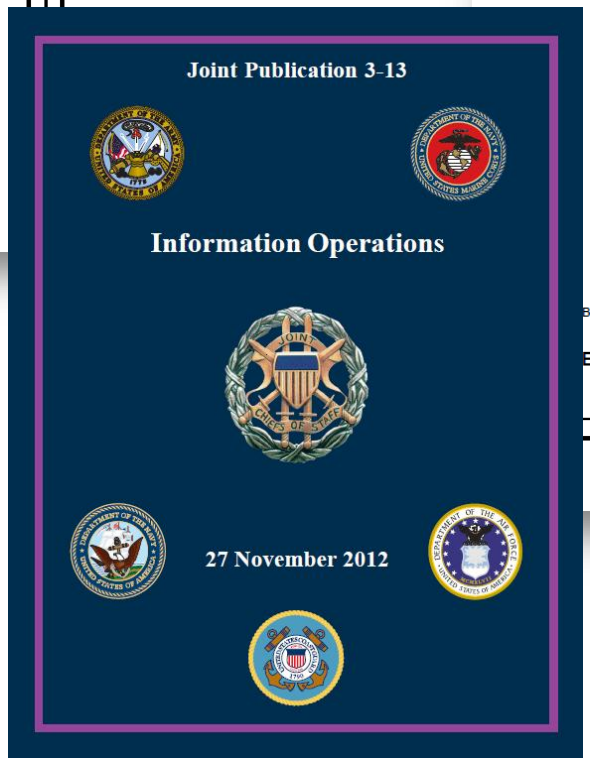
Sources



Committee on National Security Systems

CNSS Instruction No. 4009
26 April 2010

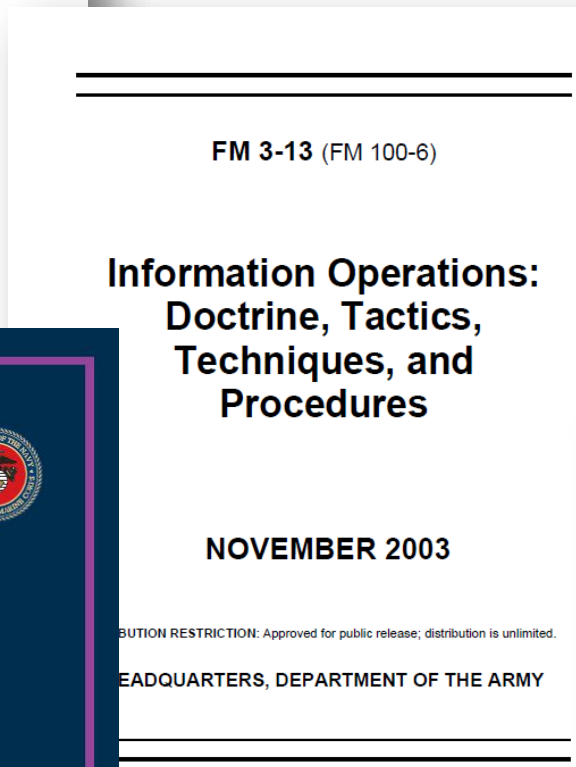
National
Information Assurance (IA)
Glossary



Joint Publication 3-13

Information Operations

27 November 2012



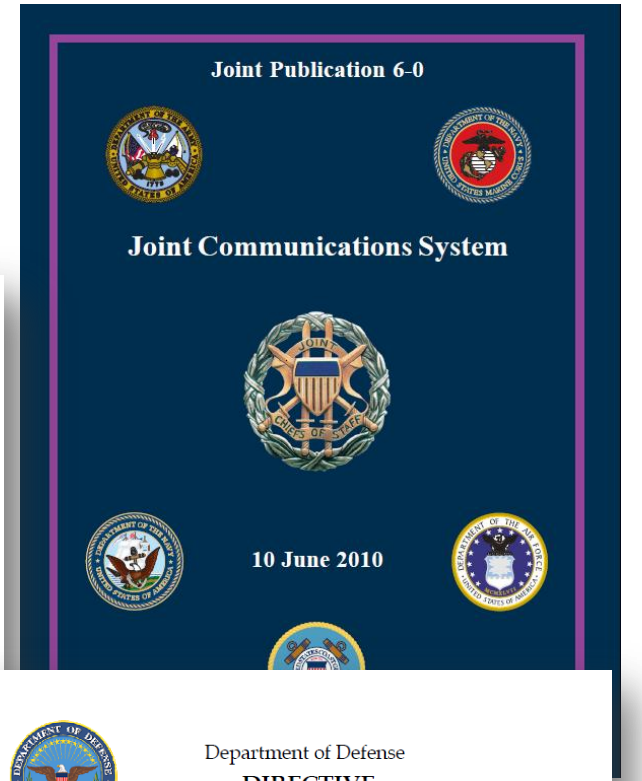
FM 3-13 (FM 100-6)

Information Operations: Doctrine, Tactics, Techniques, and Procedures

NOVEMBER 2003

BUTION RESTRICTION: Approved for public release; distribution is unlimited.

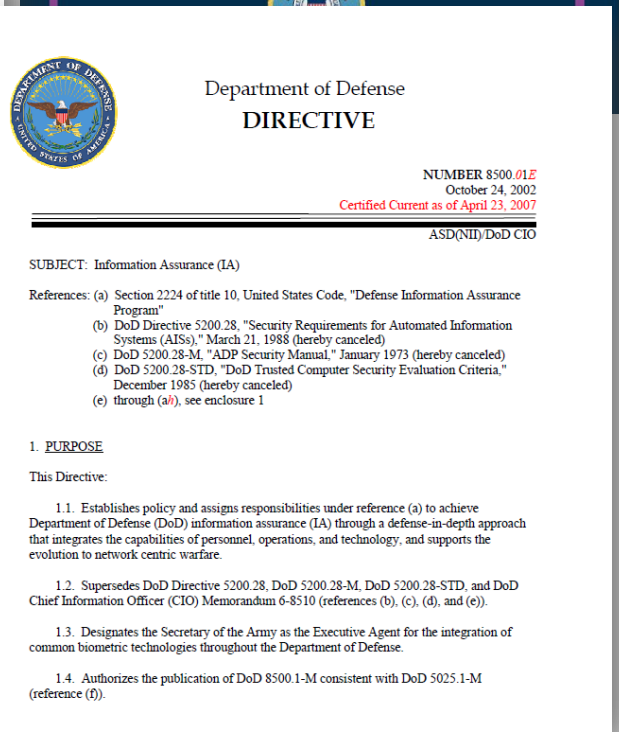
EADQUARTERS, DEPARTMENT OF THE ARMY



Joint Publication 6-0

Joint Communications System

10 June 2010



Department of Defense
DIRECTIVE

NUMBER 8500.01E
October 24, 2002
Certified Current as of April 23, 2007

ASD(NII)/DoD CIO

SUBJECT: Information Assurance (IA)

References: (a) Section 2224 of title 10, United States Code, "Defense Information Assurance Program"
(b) DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988 (hereby canceled)
(c) DoD 5200.28-M, "ADP Security Manual," January 1973 (hereby canceled)
(d) DoD 5200.28-STD, "DoD Trusted Computer Security Evaluation Criteria," December 1985 (hereby canceled)
(e) through (ai), see enclosure 1

1. PURPOSE

This Directive:

1.1. Establishes policy and assigns responsibilities under reference (a) to achieve Department of Defense (DoD) information assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare.

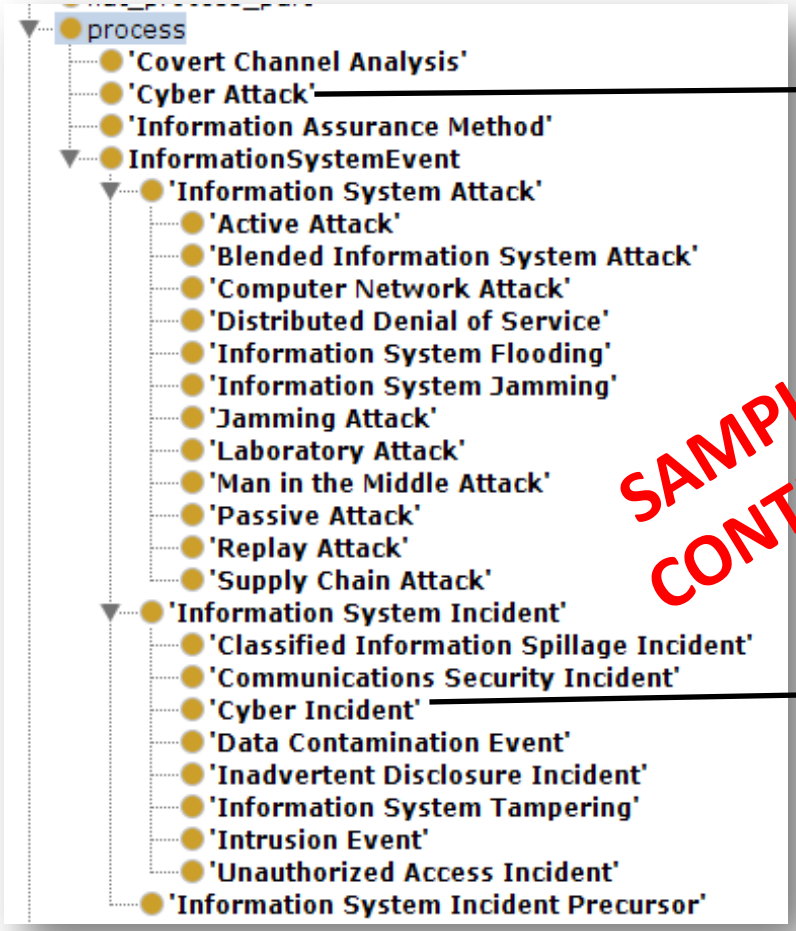
1.2. Supersedes DoD Directive 5200.28, DoD 5200.28-M, DoD 5200.28-STD, and DoD Chief Information Officer (CIO) Memorandum 6-8510 (references (b), (c), (d), and (e)).

1.3. Designates the Secretary of the Army as the Executive Agent for the integration of common biometric technologies throughout the Department of Defense.

1.4. Authorizes the publication of DoD 8500.1-M consistent with DoD 5025.1-M (reference (f)).

Well Formed Taxonomies

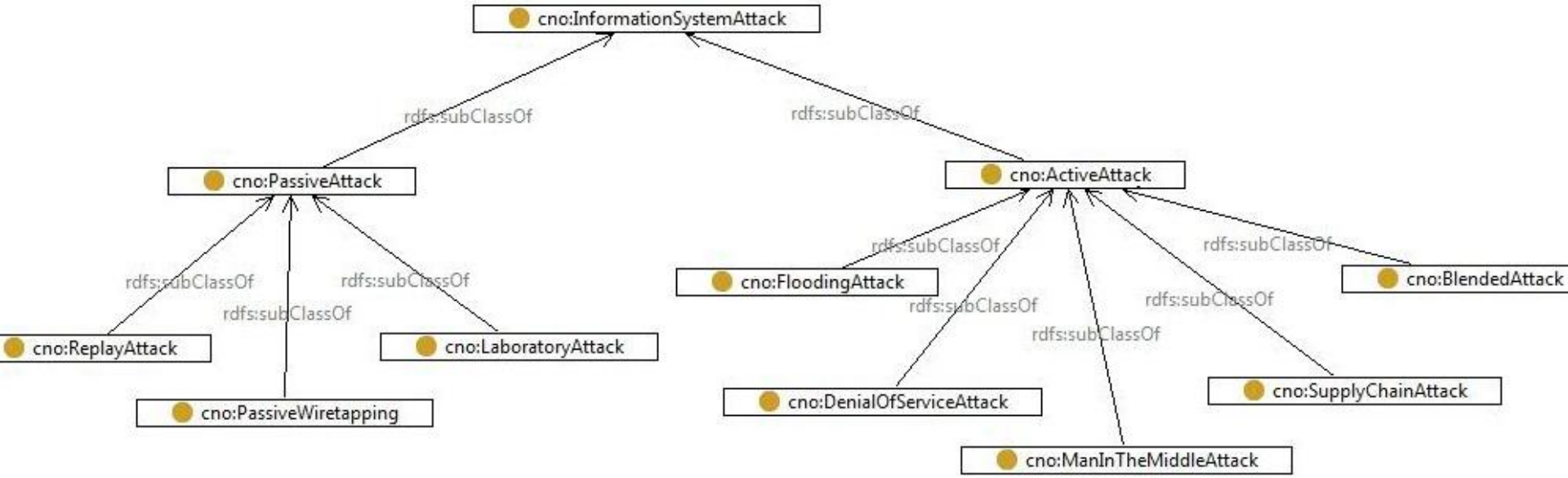
Information System Related Processes



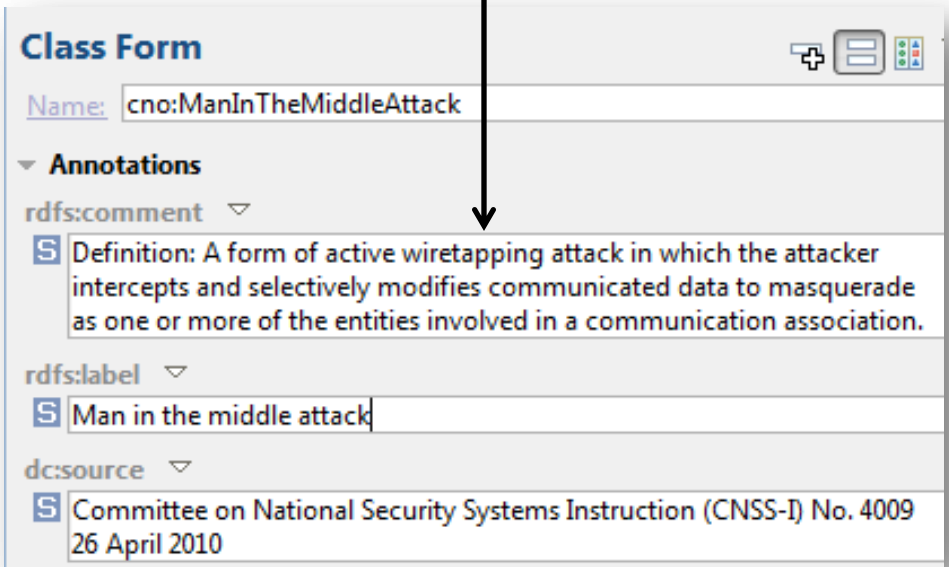
An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. (National Information Assurance Glossary)

Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein. See incident. (National Information Assurance Glossary)

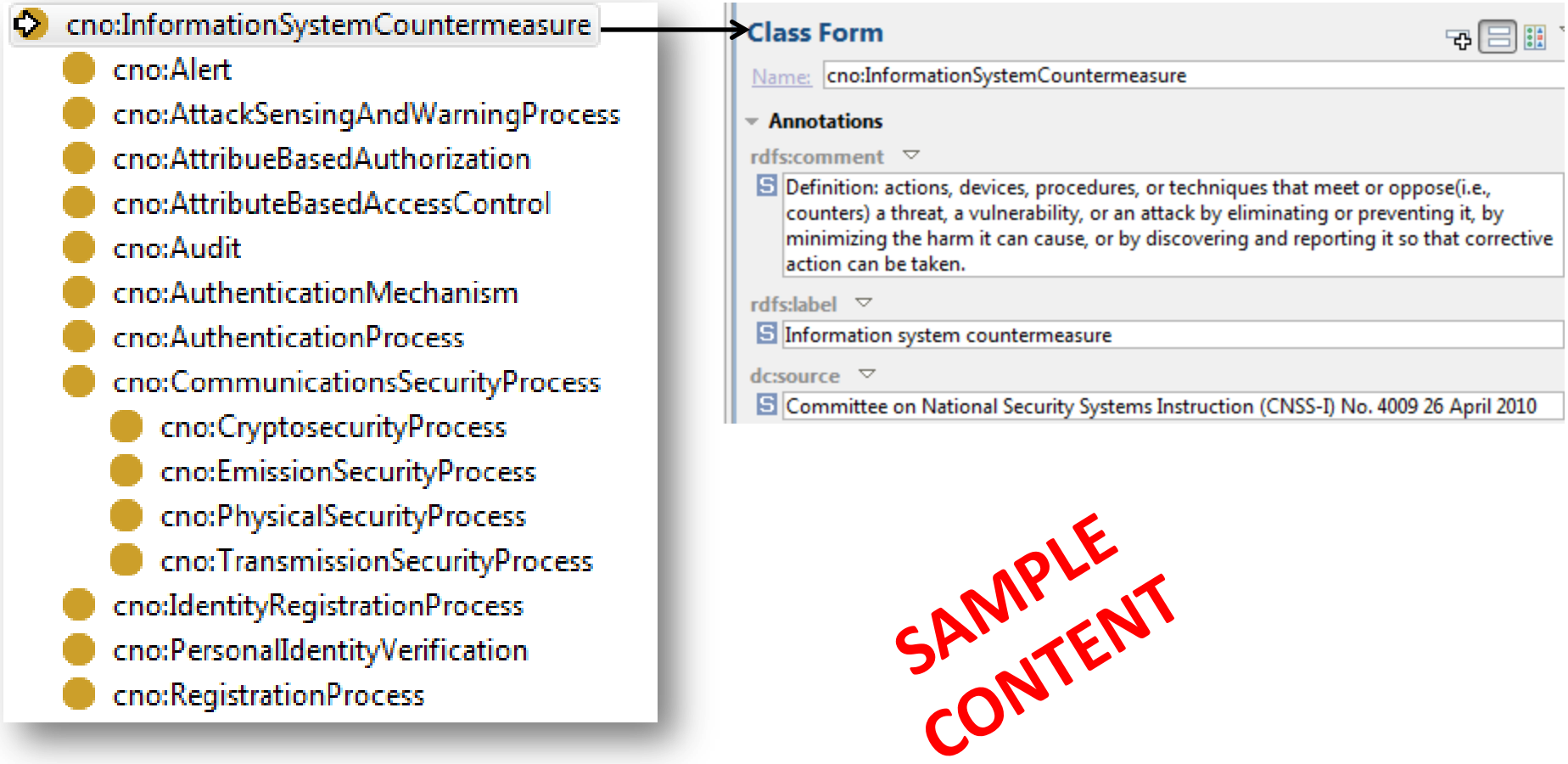
Information System Attack



SAMPLE CONTENT

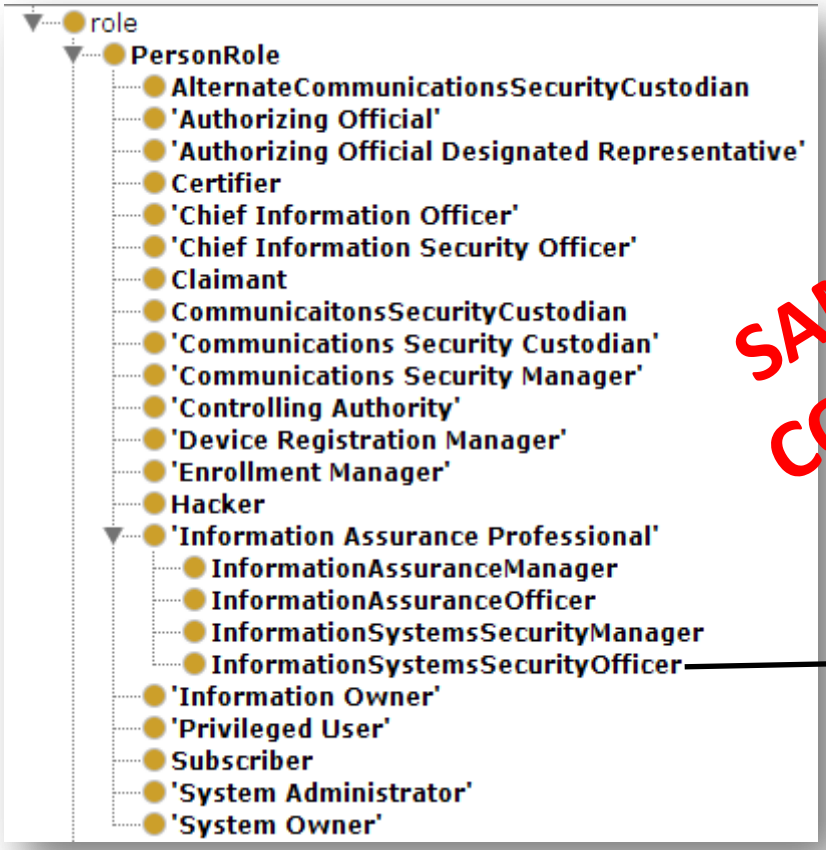


Information System Countermeasure



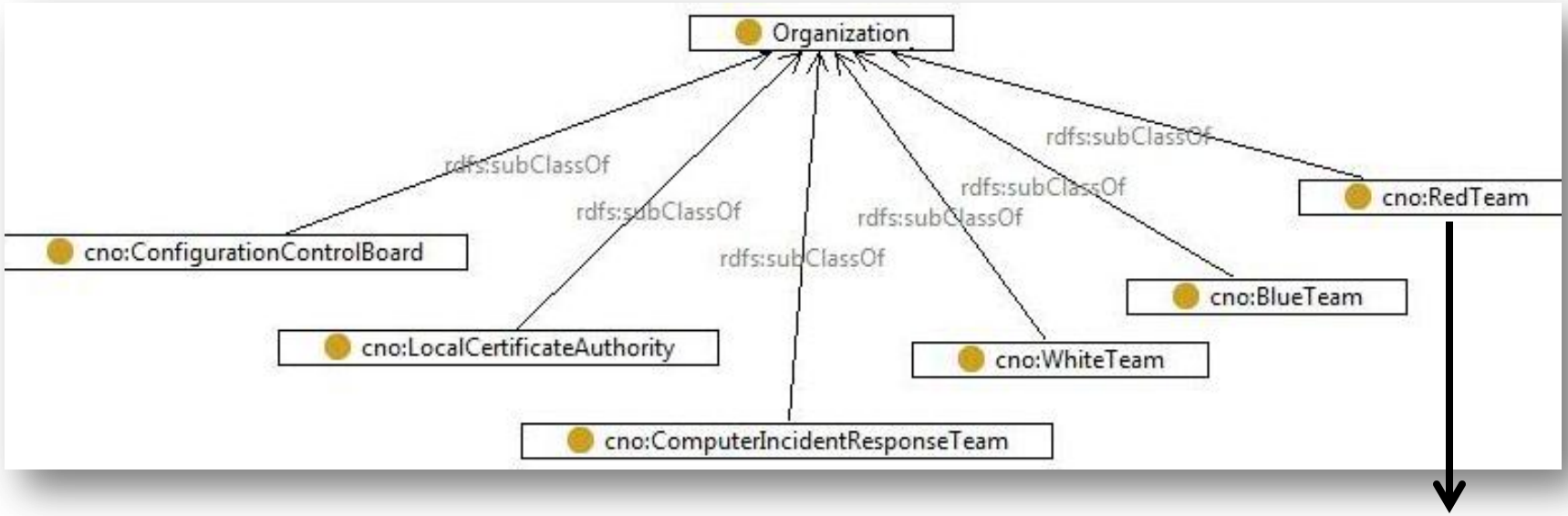
SAMPLE CONTENT

Person Roles



SAMPLE CONTENT

Individual responsible for the information assurance of a program, organization, system, or enclave.



SAMPLE CONTENT

Class Form

Name: cno:RedTeam

Annotations

rdfs:comment

S Definition: A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise Information Assurance by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment.

rdfs:label

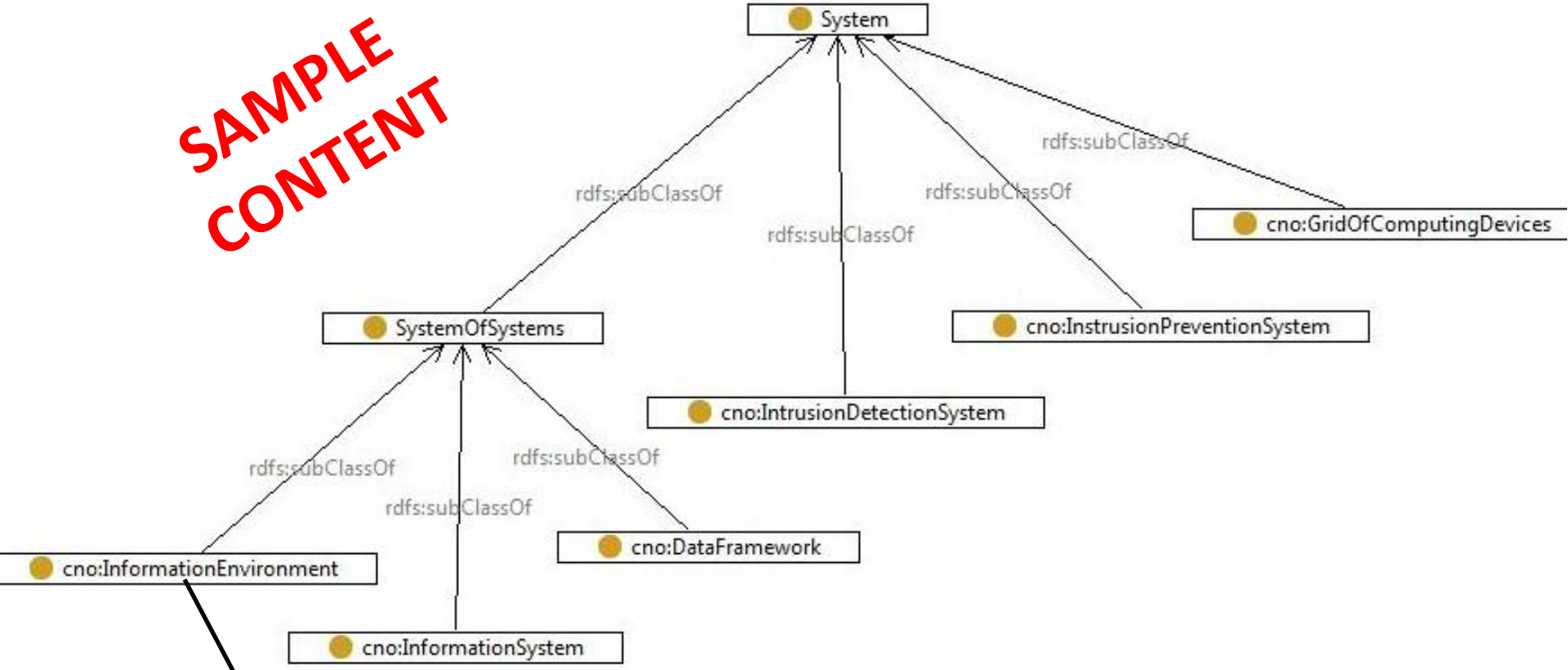
S Red team

dc:source

S Committee on National Security Systems Instruction (CNSS-I) No. 4009 26 April 2010

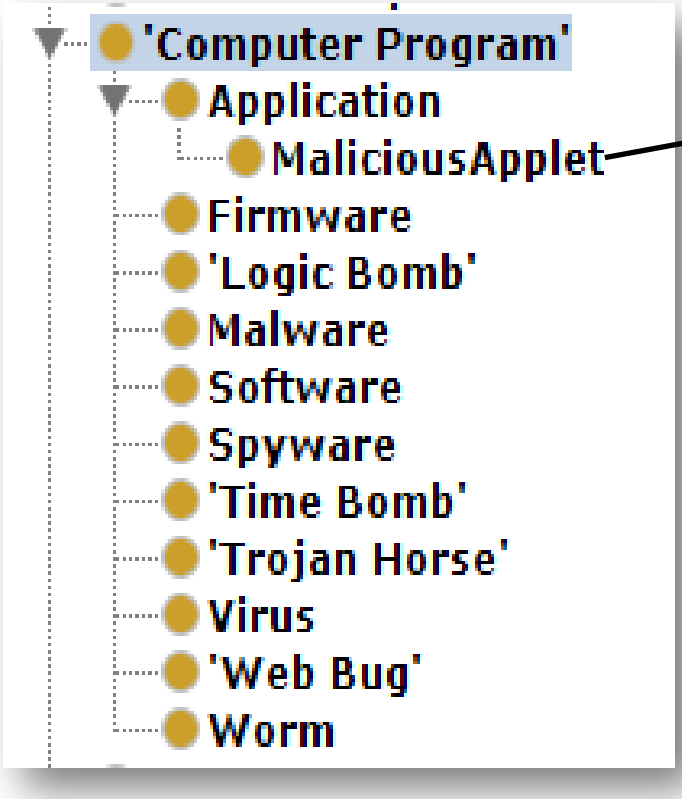
Systems

SAMPLE CONTENT



Definition: Aggregate of individuals, organizations, and/or systems that collect, process, or disseminate information, also included is the information itself. (JP 3-13 Joint Information Operations)

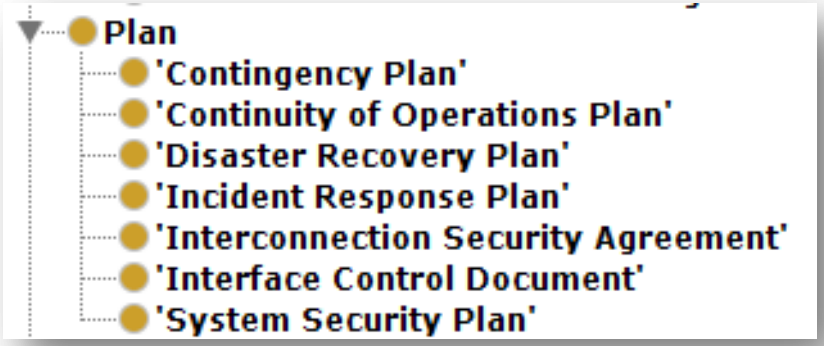
Computer Programs

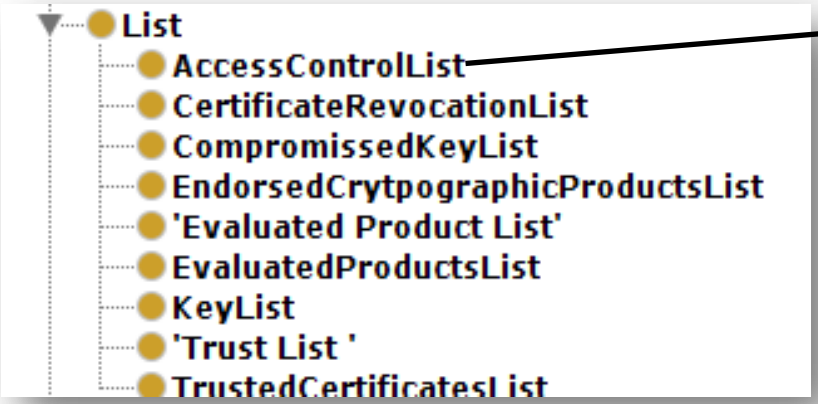


Small application programs that are automatically downloaded and executed and that perform an unauthorized function on an information system. (JP 3-13)

SAMPLE CONTENT

Information Content Entities





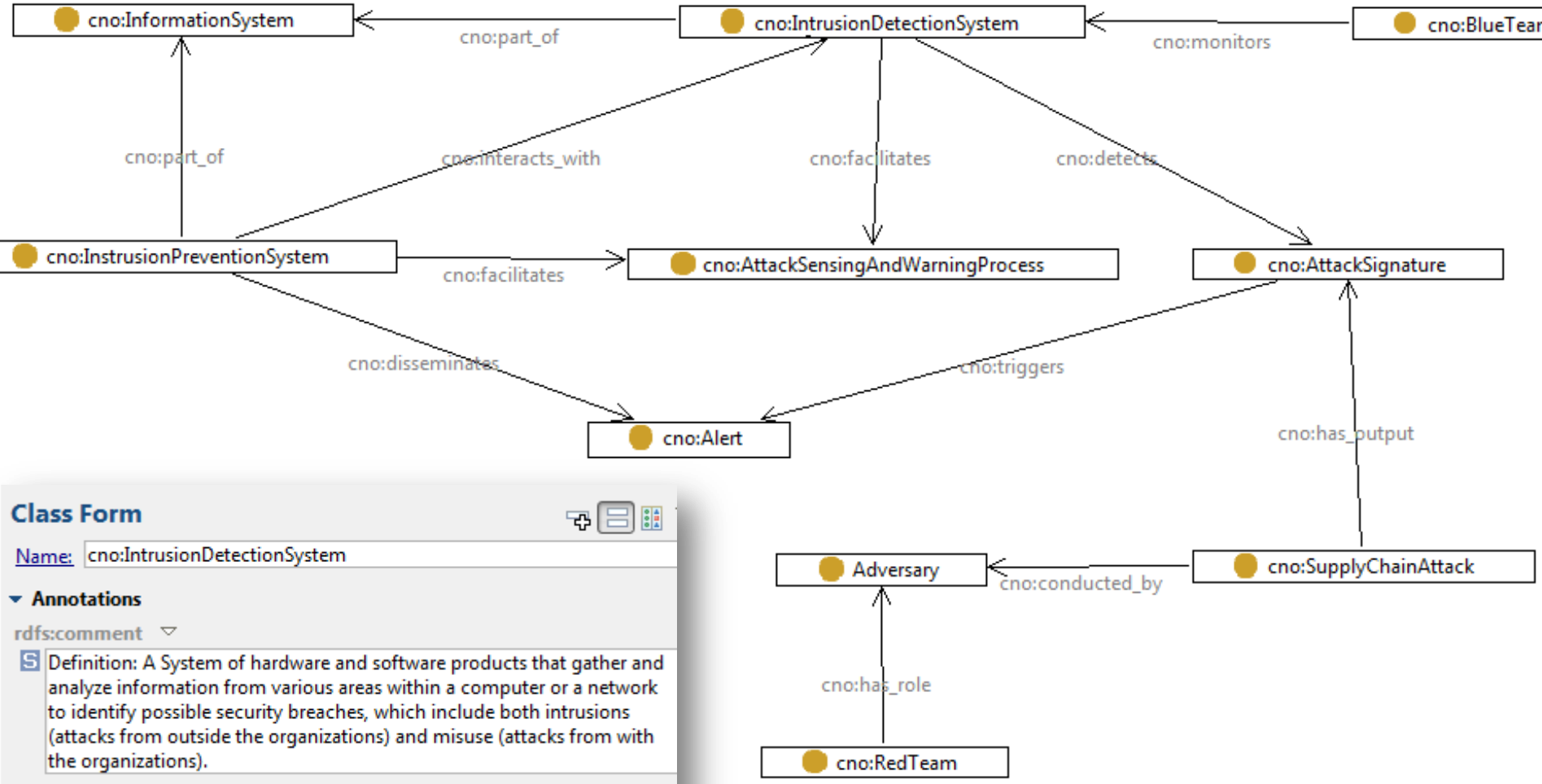
SAMPLE CONTENT

1. A list of permissions associated with an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object.

2. A mechanism that implements access control for a system resource by enumerating the system entities that are permitted to access the resource and stating, either implicitly or explicitly, the access modes granted to each entity.

Integrating Taxonomies

Intrusion Detection System



Class Form

Name: cno:IntrusionDetectionSystem

Annotations

rdfs:comment

Definition: A System of hardware and software products that gather and analyze information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from with the organizations).

rdfs:label

Intrusion detection system

dc:source

Committee on National Security Systems Instruction (CNSS-I) No. 4009 26 April 2010

Registration Process

Class Form

Name: cno:RegistrationProcess

Annotations

rdfs:comment

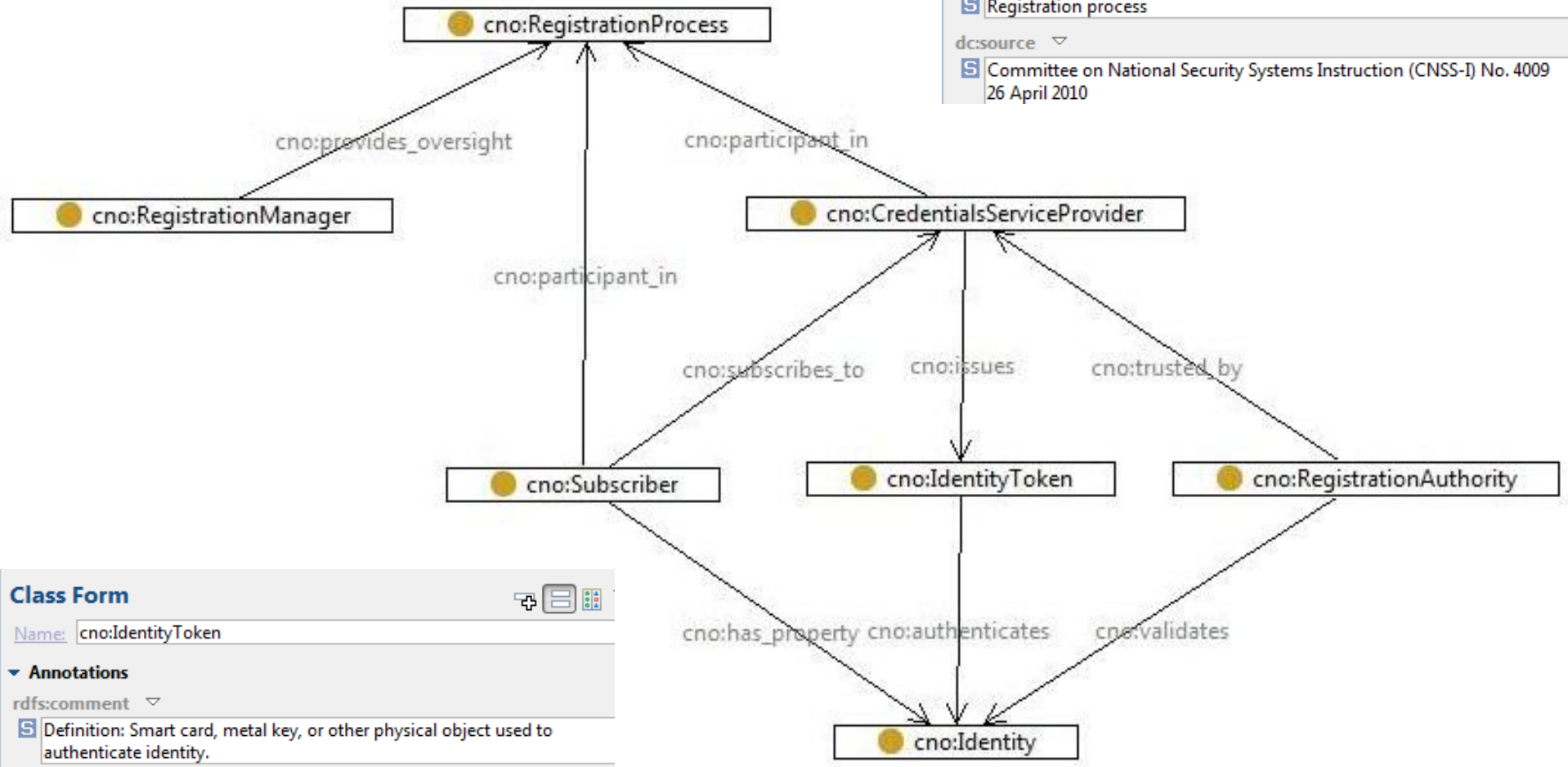
S The process through which a party applies to become a subscriber of a Credentials Service Provider (CSP) and a Registration Authority validates the identity of that party on behalf of the CSP.

rdfs:label

S Registration process

dc:source

S Committee on National Security Systems Instruction (CNSS-I) No. 4009 26 April 2010



Class Form

Name: cno:IdentityToken

Annotations

rdfs:comment

S Definition: Smart card, metal key, or other physical object used to authenticate identity.

rdfs:label

S Identity token

dc:source

S Committee on National Security Systems Instruction (CNSS-I) No. 4009 26 April 2010

Cyber Security Use Case
(next 4 slides)

- Cyber Threat Analyst
- Participates in Cyber Threat Detection Process
- Authors Cyber Incident Report
- Authors Cyber Forensics Report
- Shares with Trusted Partners

Cyber Incident

instance_of

Suspected Phishing Incident 132422MAR13

has_objective

Cyber Threat Analysis Process

followed_by

Cyber Threat Detection Process

participates_in

Cyber Threat Analyst

has_role

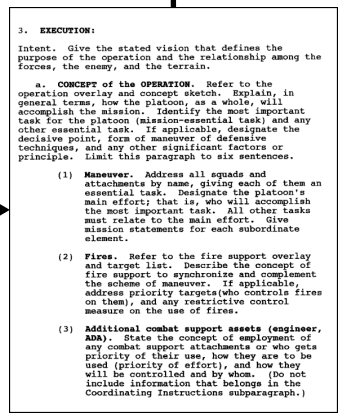
author_of

Cyber Incident Report

is_a

Initial Cyber Incident Report

instance_of



3. **EXECUTION:**

Intent. Give the stated vision that defines the purpose of the operation and the relationship among the forces, the enemy, and the terrain.

a. **CONCEPT of the OPERATION.** Refer to the operation overlay and concept sketch. Explain, in general terms, how the platoon, as a whole, will accomplish the mission. Identify the most important task for the platoon (mission-essential task) and any other essential task. If applicable, designate the decisive point, form of maneuver of defensive techniques, and any other significant factors or principle. Limit this paragraph to six sentences.

(1) **Maneuver.** Address all squads and attachments by name, giving each of them an essential task. Designate the platoon's main effort; that is, who will accomplish the most important task. All other tasks must relate to the main effort. Give mission statements for each subordinate element.

(2) **Fires.** Refer to the fire support overlay and target list. Describe the concept of fire support to synchronize and complement the scheme of maneuver. If applicable, address priority targets(who controls fires on them), and any restrictive control measure on the use of fires.

(3) **Additional combat support assets (engineer, ADA).** State the concept of employment of any combat support attachments or who gets priority of their use, how they are to be used (priority of effort), and how they will be controlled and by whom. (Do not include information that belongs in the Coordinating Instructions subparagraph.)

Initial Cyber Incident Report 22 March 2013

Cyber Threat Detection & Analysis Process

Cyber Threat Analysis Process

followed_by

Cyber Threat Detection Process

Cyber Incident

instance_of

Suspected Phishing Incident 132422MAR13

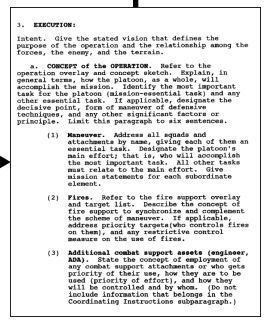
has_target

participates_in

Cyber Threat Analyst

author_of

Initial Cyber Incident Report 22 March 2013



3. **EXECUTION:**

Intent. Give the stated vision that defines the purpose of the operation and the relationship among the forces, the enemy, and the terrain.

a. **CONCEPT of the OPERATION.** Refer to the operation overlay and concept sketch. Explain, in general terms, how the platoon, as a whole, will accomplish the mission. Identify the most important task for the platoon (mission-essential task) and any other essential task. If applicable, designate the decisive point, form of maneuver of defensive techniques, and any other significant factors or principle. Limit this paragraph to six sentences.

(1) **Maneuver.** Address all squads and attachments by name, giving each of them an essential task. Designate the platoon's main effort; that is, who will accomplish the most important task. All other tasks must relate to the main effort. Give mission statements for each subordinate element.

(2) **Fires.** Refer to the fire support overlay and target list. Describe the concept of fire support to synchronize and complement the scheme of maneuver. If applicable, address priority targets(who controls fires on them), and any restrictive control measure on the use of fires.

(3) **Additional combat support assets (engineer, ADA).** State the concept of employment of any combat support attachments or who gets priority of their use, how they are to be used (priority of effort), and how they will be controlled and by whom. (Do not include information that belongs in the Coordinating Instructions subparagraph.)

Cyber Incident Report

is_a

Initial Cyber Incident Report

instance_of

Confirmed Cyber Incident Forensic Process

Cyber Incident Indicator Pattern

has_output

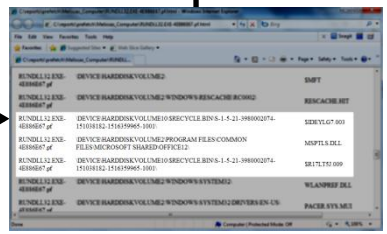
Confirmed Phishing Incident 132422MAR13

Cyber Threat Forensic Process

participates_in

Cyber Threat Analyst

author_of



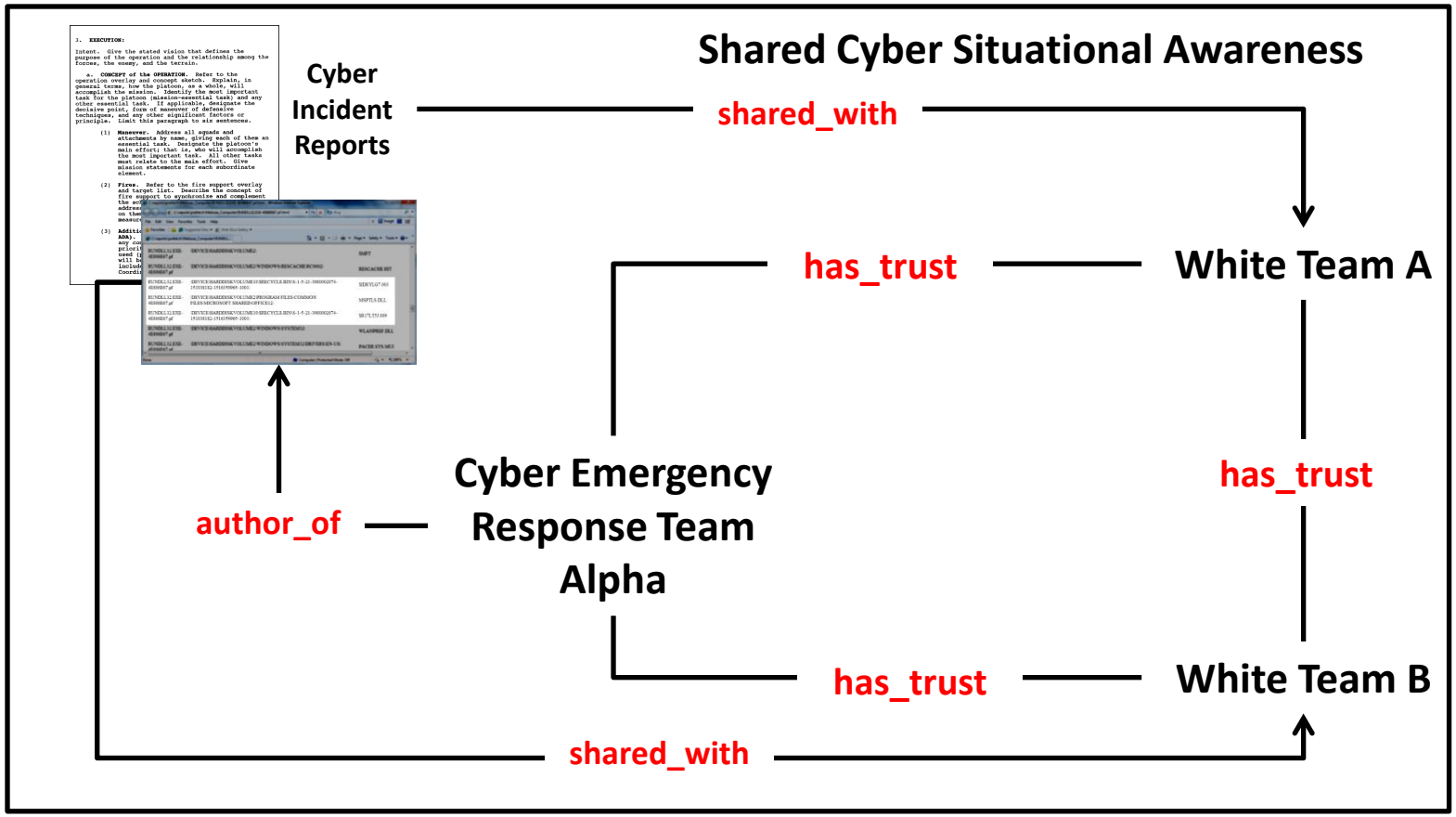
Cyber Incident Forensic Report 22 March 2013

instance_of

Cyber Incident Forensic Report

is_a

Cyber Incident Report


Shared Cyber Situational Awareness
Cyber Incident Reports
shared_with
has_trust
White Team A
Cyber Emergency Response Team Alpha
author_of
has_trust
has_trust
White Team B
shared_with

Conclusion

- Avoid Mass Terms (e.g. Data or Computing)
- Use Individual Nouns (e.g. Data Set or Computing Process)
- Distinguish
  - Strict “is_a” taxonomy
    - cat ***is_a*** mammal
    - storm ***is_a*** weather event
    - computer disk ***is_a*** information bearing entity
  - Diagram
    - Network Diagram
    - Tree Diagram
    - System Diagram